IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

UNITED STATES OF AMERICA	§	**SEALED**
	§	
v.	§	CASE NUMBER 4:16-CR-00111-ALM-CAN
	§	
JOSE VICTOR HERNANDEZ-CUELLAR	§	

REPORT AND RECOMMENDATION
OF UNITED STATES MAGISTRATE JUDGE

Pending before the Court are Defendant Jose Hernandez-Cuellar's ("Defendant") Motion to Suppress Evidence ("Motion to Suppress") [Dkt. 25] and Opposed Motion Requesting Evidentiary Hearing ("Motion for Evidentiary Hearing") [Dkt. 41] (collectively the "Motions"). On March 14, 2017, the undersigned conducted a hearing and heard oral argument from both the Government and Defendant on the pending Motions. After considering the Motions, all relevant filings and evidence, as well as the oral argument of counsel at hearing, the Court recommends that Defendant's Motion to Suppress [Dkt. 25] and Motion for Evidentiary Hearing [Dkt. 41] each be **DENIED**.[1]

BACKGROUND

On September 7, 2016, Defendant was indicted for a violation of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography) [Dkt. 11]. The indictment charges that Defendant "did employ, use, persuade, induce, entice, and coerce . . . a minor . . . to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, using a Canon PowerShot A400 digital camera, containing a SanDisk 128MB SD card, bearing serial AK04351VZ" [Dkt. 11].

[1] Defendant also filed a Motion to Continue Suppression Hearing ("Motion to Continue") [Dkt. 40]. The Court recommends Defendant's Motion to Continue [Dkt. 40] be denied as moot. To the extent Defendant seeks through the Motion to Continue to introduce evidence not presently on the record for the Court's review, the Court construes Defendant's Motion for Evidentiary Hearing as inclusive of such request [*see* Dkt. 41 (requesting evidentiary hearing on Motion to Suppress)].

The charges against Defendant stem from the seizure of evidence at his home resulting from investigation into his alleged activity on Website A (also known as "Playpen"), which the FBI has described as "a message board website whose primary purpose is the advertisement and distribution of child pornography" [Dkt. 25, Ex. 2 at 13].

I. THE FBI INVESTIGATION INTO WEBSITE A AND THE NIT WARRANT

In late 2014 to early 2015, the FBI discovered and accessed Website A through a Tor-enabled web browser,[2] acting on information provided by a foreign law enforcement agency [Dkt. 25, Ex. 2 at 13, 21]. As a "hidden service," users could access Website A only if they knew (or ventured the highly unlikely guess at) Website A's precise URL—"a series of algorithm-generated characters, such as 'asdlk8fs9dflku7f' followed by the suffix '.onion'"—which, incidentally, Website A's administrator routinely changed [Dkt. 25, Ex. 2 at 12-13 & 13 n.3]. Website A was believed to have "been operating since approximately August 2014" and to have "contain[ed] a total of 95,148 posts, 9,333 total topics, and 158,094 total members" [Dkt. 25, Ex. 2 at 13]. The main page of Website A and the various sections and forum titles contained therein (such as "Jailbait – Boy," "Jailbait – Girl," "Preteen – Boy," and "Preteen – Girl") made clear the site's content centered on child pornography [Dkt. 25, Ex. 2 at 13, 15-17]. The FBI's "review of topics within the . . . forums revealed the majority contained discussions, as well as numerous images that appeared to depict child pornography . . . and child erotica of prepubescent females, males, and toddlers" [Dkt. 25, Ex. 2 at 17-18].

[2] "Tor" stands for "The Onion Router," an anonymity network initially developed by the U.S. Naval Research Laboratory that now is publicly available and accessible [Dkt. 25, Ex. 2 at 11; *see also* http://www.torproject.org/about/overview.html.en]. Tor networks actively conceal a user's identity by routing the interactions between the user's computer and a target website through a series of "nodes"—other locations on the Internet with distinct IP addresses [Dkt. 25 at 10-12]. Users access websites through Tor networks with both good intentions, *see, e.g.*, http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html (noting "Peaceniks and human rights groups, . . . journalists, private citizens and the military" use Tor), and bad, *see, e.g.*, http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (reporting that "[m]ore than four out of five Tor hidden services site visits were to online destinations with pedophilia materials").

Acting on the foreign tip, the FBI seized the Website A server from North Carolina pursuant to a warrant on February 20, 2015, then delivered the server to the Eastern District of Virginia, where it operated the server [Dkt. 25, Ex. 1 at 19]. The FBI then obtained another warrant from a magistrate judge in the Eastern District (the "Eastern District of Virginia Magistrate") authorizing the FBI to deploy a "Network Investigative Technique" (a "NIT") on the Website A server to "attempt to identify the actual IP addresses and other identifying information of computers used to access 'Website A'" (hereinafter the "NIT Warrant") [Dkt. 25, Ex. 1 at 19; *see also* Dkt. 25, Ex. 2 at 24 (defining those computers that access Website A as "activating computers")]. The NIT "[was] designed to cause the [activating] computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its locations, other information about the computer, and the user of the computer accessing 'Website A'" [Dkt. 25, Ex. 1 at 19; *see also* Dkt. 25, Ex. 2 at 24]. Specifically, the NIT would cause activating computers to send to the Government-controlled computer the seven pieces of information identified in Attachment B to the NIT Warrant [Dkt. 25, Ex. 1 at 2]. Attachment A specifies the "place to be searched," and Agent MacFarlane's Affidavit further clarifies the NIT's function as well as the search and seizure mechanisms the NIT employs [Dkt. 25, Ex. 2 at 1, 23-27, 29-30]. The FBI operated Website A's server and deployed NITs in this manner until "approximately March 4, 2015" [Dkt. 25, Ex. 1 at 19].

II. THE RESIDENTIAL SEARCH WARRANT & INVESTIGATION INTO "ZAPATERO5"

On November 5, 2015, Special Agent Christopher Thompson ("Agent Thompson") of the Federal Bureau of Investigation, Child Exploitation Task Force, presented a search warrant application and affidavit in support of a residential search warrant (the "Residential Warrant" and "Residential Affidavit") [E.D. Tex. Case No. 4:15-MJ-433, Dkt. 1]. The Residential Warrant

sought authorization to search Defendant's home for items and information "pertaining to the transportation, receipt, distribution, or possession of child pornography, . . . or . . . visual depictions of minors engaged in sexually explicit conduct" in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2) [Dkt. 25, Ex. 1]. The Residential Affidavit, prepared by Agent Thompson, describes Agent Thompson's credentials, provides information and definitions pertaining to child pornography and computers, and outlines the FBI's background investigation of Website A, which the Government alleges Defendant used to engage in the exploitation of children [Dkt. 25, Ex. 1]. The Residential Warrant was issued on the basis of the Affidavit, which relied heavily upon the FBI's underlying investigation into Website A to establish probable cause.[3]

According to the Residential Affidavit, the user "zapatero5," whom the FBI later identified as Defendant, "originally registered an account on 'Website A' on December 14, 2014" [Dkt. 25, Ex. 1 at 20]. The Residential Affidavit indicates that, between December 14, 2014, and March 5, 2015, zapatero5 "had been actively logged into [Website A] for a total of approximately 28 hours and 31 minutes" [Dkt. 25, Ex. 1 at 20]. Specifically, zapatero5 is alleged to have accessed Website A at least three times between February 28, 2015 and March 2, 2015, to view or download images of nude toddler females engaged in sexual activities (such as sex with an adult male), according to the Residential Affidavit [Dkt. 25, Ex. 1 at 20-22].

Using the NIT, the FBI discovered Defendant's true IP address, obtained an administrative subpoena, served the subpoena on Defendant's service provider, and thereby determined the precise location of Defendant's computer [Dkt. 25, Ex. 1 at 20-23]. The FBI then obtained and executed the Residential Warrant [Dkt. 38 at 7]. The FBI encountered Defendant while executing

[3] The Court notes Defendant does not challenge the Residential Warrant itself. Rather, Defendant challenges the Residential Warrant only to the extent it relies upon the fruits of the NIT Warrant to establish probable cause. Defendant concedes that, if the Court finds the NIT Warrant valid and legal, then the Residential Warrant would be facially valid, as well [Dkt. 46 at 3].

the Residential Warrant, and Defendant "spoke with the agents and admitted that he had viewed child pornography, that he had used Tor, that he utilized the screen name 'zapatero5,' [and] that he had used specific search terms to locate child pornography" [Dkt. 38 at 7]. Defendant also "identified files that he had downloaded or seen on his computer before" [Dkt. 38 at 7]. In addition, the FBI located "images depicting the exhibition of the genitals of prepubescent males who were known to [Defendant]" [Dkt. 38 at 7]. The Affidavit indicates Defendant, after being advised of his *Miranda* rights, identified a prepubescent male in certain of the seized images as a person to whom Defendant had access and whom Defendant photographed [Dkt. 2]. As noted, Defendant was subsequently indicted on September 7, 2016, for a violation of 18 U.S.C. § 2251(a), (e) (Production of Child Pornography) [Dkt. 11]. Defendant filed the Motion to Suppress on December 30, 2016, seeking suppression of "all evidence, including statements, computers and digital images, seized from [Defendant] on or about November 6, 2015 and on various dates in 2016, and pursuant to [the Residential Warrant]" [Dkt. 25 at 1]. The Government filed its Response to Defendant's Motion to Suppress on March 2, 2017 [Dkt. 38], and the Court set the matter for hearing ("Hearing") on March 14, 2017 [Dkt. 39]. On March 10, 2017, Defendant filed the Motion for Evidentiary Hearing [Dkt. 41]. The Court held Hearing on March 14, 2017 [Dkt. 45] related to both Motions, and the transcript of Hearing was filed April 26, 2017 [Dkt. 46].

ANALYSIS

Defendant moves to suppress all evidence obtained from the NIT Warrant, arguing the Eastern District of Virginia Magistrate issued the NIT Warrant without authority under Federal Rule of Criminal Procedure 41(b) and/or 28 U.S.C. § 636 (the Federal Magistrate Judges Act) and also that the NIT Warrant failed to particularize the place to be searched or the items to be seized [Dkt. 25 at 5-11]. The Parties' respective briefing assumes the Fourth Amendment applies—that

Defendant had a protected privacy interest invaded by a search and/or seizure by the Government; accordingly, the Court assumes the same for the sake of its analysis. *See United States v. Perdue*, No.3:16-CR-305-D(1), 2017 WL 661378, at *2 n.3 (N.D. Tex. Feb. 17, 2017) (assuming "*arguendo* that the NIT constituted a search that triggered the protections of the Fourth Amendment").

I. THE FOURTH AMENDMENT FRAMEWORK AND THE SUPPRESSION REMEDY

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. The exclusionary rule, which permits criminal defendants to seek exclusion (suppression) of evidence obtained through "illegal search and seizure[,]" provides one vehicle through which citizens may "effectuate [this] Fourth Amendment right . . . ." *United States v. Calandra*, 414 U.S. 338, 347 (1974) (noting that this rule "applies as well to the fruits of the illegally seized evidence"). The U.S. Supreme Court has characterized exclusion through suppression for decades as an "extreme sanction" that courts should apply only sparingly. *United States v. Leon*, 468 U.S. 897, 926 (1984); *see also Herring v. United States*, 555 U.S. 135, 141 (2009) (warning that application of the exclusionary rule exacts "substantial social costs") (citations and internal quotations omitted); *Hudson v. Michigan*, 547 U.S. 586, 591 (2006) ("Suppression of evidence, however, has always been our last resort, not our first impulse."). Further, "[a] defendant normally bears the burden of proving by a preponderance of the evidence that the challenged search or seizure was unconstitutional." *United States v. Waldrop*, 404 F.3d 365, 368 (5th Cir. 2005).

A court must engage in a two-part inquiry in deciding whether to suppress evidence: it generally must ask first whether the good faith exception applies (and, in turn, whether any of the exceptions to that rule applies) and then, if that rule does not apply and the situation presents "an

important Fourth Amendment question[,]" whether probable cause supports the warrant in question. *Leon*, 468 U.S. at 924 ("[C]ourts could reject suppression motions . . . by turning immediately to a consideration of the officers' good faith."); *see also United States v. Stalnaker*, 571 F.3d 428, 436 (5th Cir. 2009). "Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith." *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003) (citing *Leon*, 468 U.S. 897). "The 'good faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization.'" *United States v. Pope*, 467 F.3d 912, 916 (5th Cir. 2006) (quoting *Leon*, 568 U.S. at 922 n.23). Normally, the issuance of a warrant by a magistrate suffices to establish an officer's good faith. *United States v. Pena-Rodriquez*, 110 F.3d 1120, 1130 (5th Cir. 1997). But good faith cannot be established if one of the following four circumstances is present:

> (1) [i]f the issuing magistrate/judge was misled by information in an affidavit that the affiant knew was false or would have known except for reckless disregard of the truth; (2) where the issuing magistrate/judge wholly abandoned his or her judicial role; (3) where the warrant is based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that the executing officers cannot reasonably presume it to be valid.

Payne, 341 F.3d at 399-400 (quoting *United States v. Webster*, 960 F.2d 1301, 1307 n.4 (5th Cir. 1992)) (hereinafter referred to as the "*Leon* exceptions"). In considering whether the good-faith exception applies, the Court does not attempt to determine the officers' subjective belief regarding the validity of the warrant. *See Leon*, 468 U.S. at 922 n.23. Rather, the Court's inquiry is "confined to the objectively ascertainable question of whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* Within this

framework, a court must consider first whether the good faith exception or any of the *Leon* exceptions apply; courts consider whether probable cause supports the warrant only in the absence of good faith. *See Stalnaker*, 571 F.3d at 436; *United States v. Craig*, 861 F.2d 818, 820 (5th Cir. 1988) ("Principles of judicial restraint and precedent dictate that, in most cases, we should not reach the probable cause issue if . . . the good-faith exception of *Leon* will resolve the matter.").

Because the good faith exception only becomes relevant where a magistrate issues a "warrant later determined to be deficient[,]" the Court turns first to consider Defendant's arguments that the NIT Warrant constitutes an improper general warrant and/or that the Eastern District of Virginia Magistrate issued the NIT Warrant without authority under Rule 41 and/or § 636. *See Payne*, 341 F.3d at 399 (citing *Leon*, 468 U.S. at 921-25).

II. NIT WARRANT PARTICULARITY

Defendant argues the NIT Warrant suffers from a lack of particularity that renders it unconstitutional [Dkt. 25 at 12-14]. Specifically, Defendant asserts the NIT Warrant "erroneously describe[s] the place to be searched as the [Website A] server, located in Virginia" and that it improperly "describe[s] the information to be seized as data from the activating computers while overlooking the fact that such information could only be obtained by first searching and seizing the data from those computers" [Dkt. 25 at 13]. Defendant contends that the officers' execution of the NIT Warrant outside of the Eastern District of Virginia despite the clear limits on the Eastern District of Virginia Magistrate's authority to issue such a wide-ranging warrant illustrates "that the description [contained in the NIT Warrant is] insufficient to prevent a reasonable probability of mistake" [Dkt. 25 at 13].

General warrants—those that permit "a general, exploratory rummaging of a person's belongings"—"are prohibited by the Fourth Amendment." *Andresen v. Maryland*, 427 U.S. 463,

479 (1976). The Fourth Amendment instead requires "particular" warrants: a warrant that "'would permit an executing officer to reasonably know what items are to be seized.'" *United States v. Layne*, 43 F.3d 127, 132-33 (5th Cir. 1995) (quoting *United States v. Beaumont*, 972 F.2d 553, 560 (5th Cir. 1992)). Warrants are sufficiently particular where "the executing officer is left with no discretion to decide what may be seized." *United States v. Allen*, 625 F.3d 830, 834-35 (5th Cir. 2010) (citation and internal quotations omitted). Courts look to the warrant's language to determine whether the warrant gave the executing officers discretion in determining what places should be searched or what items should be seized. *See Williams*, 806 F.2d at 598. But "[t]he law permits an affidavit incorporated by reference to amplify particularity, notwithstanding that, by its terms, the Fourth Amendment 'requires particularity in the warrant, not in the supporting documents.'" *United States v. Triplett*, 684 F.3d 500, 505 (5th Cir. 2012) (quoting *Groh v. Ramirez*, 540 U.S. 551, 557-58 (2004)). Further, even "generic language is permissible if it particularizes the type of items to be seized." *United States v. Kimbrough*, 69 F.3d 723, 727 (5th Cir. 1995). Courts have found warrants to be general only in limited circumstances, such as where the warrants "merely repeated the language of the statute[,]" *Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kansas City*, 367 U.S. 717, 731-32 (1961), completely omitted any affidavit or application and provided a vague description only of the place to be searched, *Groh*, 540 U.S. at 558, and authorized search and seizure of the instrumentalities or evidence of a crime, *Allen*, 625 F.3d at 839.

Here, the NIT Warrant itself authorizes the search "of computers that access [Website A,]" and expressly incorporates attachments and an affidavit, namely Affidavits A and B and Agent MacFarlane's Affidavit. Attachment A identifies the "place to be searched" by describing how the FBI intended to deploy the NIT onto Website A's server and how the NIT would target the

"activating computers" [Dkt. 25, Ex. 2, Attachment A]. Attachment B identifies the "information to be seized," listing seven distinct pieces of information the NIT would cause the activating computer to send back to the FBI, most notably the activating computer's true IP address [Dkt. 25, Ex. 2, Attachment B]. The NIT Warrant limits any search to Website A's server and activating computers and further states that seizure of information found thereon is appropriate because "there existed a fair probability that anyone accessing [Website A] possessed the intent to view and trade child pornography." *United States v. Matish*, 193 F. Supp. 3d 585, 609 (E.D. Va. 2016). Agent MacFarlane's Affidavit provides additional details about the NIT's function and defines the technical aspects of the computers to be searched and the information to be seized [*see* Dkt. 25, Ex. 2, Affidavit]. Notably, in the Court's research, every district court confronted with the question of whether the NIT Warrant sufficiently particularizes the place to be searched and items to be seized has found the NIT Warrant sufficiently particular. *See, e.g.*, *United States v. Taylor*, No. 2:16-cr-203-KOB-JEO-1, 2017 WL 1437511, at *11 (N.D. Ala. Apr. 24, 2017) (noting that "the court finds it difficult to imagine how much more specific the descriptions of the place to be searched and the items to be seized could have been" and finding the NIT Warrant sufficiently particular); *United States v. Pawlak*, No. 3:16-CR-306-D(1), 2017 WL 661371, at *3-4 (N.D. Tex. Feb. 17, 2017) (concluding "the NIT Warrant was not a general warrant" under Fifth Circuit and U.S. Supreme Court precedent); *United States v. Deichert*, --- F. Supp. 3d ---, 2017 WL 398370, at *5-6 (E.D.N.C. Jan. 28, 2017) (finding NIT Warrant sufficiently particular); *United States v. Vortman*, No. 16-cr-00210-TEH-1, 2016 WL 7324987, at *9 (N.D. Cal. Dec. 16, 2016) (noting "several other district courts . . . have found the NIT [W]arrant was sufficiently particular" and finding the same); *United States v. Anzalone*, 208 F. Supp. 3d 358, 368 (D. Mass. 2016) (noting that, as of September 22, 2016, "[e]very court to consider this question has found the NIT

[Warrant] sufficiently particular"). Likewise, this Court concludes that the NIT Warrant is not a general warrant; when considered alongside Attachments A and B and Agent MacFarlane's Affidavit, the NIT Warrant sufficiently particularizes the place to be searched (the activating computers through the NIT deployed on the Website A server) and the items to be seized (the seven pieces of information identified in Attachment B). *See, e.g.*, *Taylor*, 2017 WL 1437511, at *11; *Michaud*, 2016 WL 337263, at *5.

III. RULE 41 AND 28 U.S.C. § 636: VIOLATION AND CONSEQUENCES

Defendant also argues the Eastern District of Virginia Magistrate lacked authority to issue the NIT Warrant under both Rule 41(b) and 28 U.S.C. § 636 and that, absent issuance of the NIT Warrant, the Residential Warrant would never have been obtained [Dkt. 25]. The Government contends the NIT Warrant was issued in compliance with Rule 41(b)(4) and, accordingly, with § 636 [Dkt. 38].

28 U.S.C. § 636 defines the "[j]urisdiction, powers, and temporary assignment [rules]" governing United States magistrate judges. It provides in relevant part as follows:

> Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law . . . all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts[] . . . .

28 U.S.C. § 636. Federal Rule of Criminal Procedure 41(b) in turn gives a magistrate judge authority to issue a search warrant in certain defined circumstances. FED. R. CRIM. P. 41(b); *see also United States v. Torres*, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *4 (W.D. Tex. Sept. 9, 2016) (noting § 636 "incorporates by reference Federal Rule of Criminal Procedure 41(b)" in defining a magistrate's authority). The Government does not contest that Rule 41, subsections (b)(1)-(3), (5) do not apply in this case [*see* Dkt. 25 at 7-10; Dkt. 38]. Given the Parties' apparent

agreement concerning Rule 41(b)(1)-(3), (5)—i.e., that those subsections do not apply in the present case—the Court focuses its analysis on Rule 41(b)(4). Rule 41(b)(4) authorizes magistrate judges "with authority in the district . . . to issue a warrant to install within the district a tracking device" that may "track the movement of . . . property located within the district, outside the district, or both . . . ." FED. R. CRIM. P. 41(b)(4). Rule 41(a) defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a[n] . . . object." FED. R. CRIM. P. 41(a)(2)(E) (incorporating by reference 18 U.S.C. § 3117). Further, "property" as used in Rule 41 "includes . . . information." FED. R. CRIM. P. 41(a)(2)(A).

A. Compliance with Rule 41(b)(4)

The Government urges the Court to find the Eastern District of Virginia Magistrate had jurisdiction under Rule 41(b)(4) to issue the NIT Warrant because the NIT constitutes a "tracking device" that the FBI "installed" in the Eastern District of Virginia [Dkt. 38 at 10-11 (asserting the FBI "deployed the NIT alongside Playpen's digital content on the government-controlled server, which was located within the Eastern District of Virginia")]. Indeed, the Government analogizes the NIT to a transmitter that affixed itself to Defendant when he made a virtual trip to the Eastern District of Virginia to access Website A's server [Dkt. 38 at 9-11]. Specifically, the Government contends the FBI installed the NIT—a set of computer instructions—onto Website A content in the Eastern District of Virginia, and that, when Defendant accessed that content, he took the (pre-installed) NIT with him [Dkt. 38 at 11]. Defendant contends to the contrary that the NIT installed itself on Defendant's computer in the Eastern District of Texas [Dkt. 25 at 9-10].

Nationwide, courts have split on the questions of whether the NIT constitutes a tracking device and where the FBI "installed" it within the meaning of Rule 41(b)(4). *Compare United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016)

(finding that, even had the installation occurred on the server located in Virginia, the (b)(4) "exception breaks down, because [the defendant] never controlled the government-controlled computer" on which the NIT was installed); *United States v. Croghan*, 209 F. Supp. 3d 1080, 1088 (S.D. Iowa 2016) (noting the NIT "caused a computer code to be installed on the activating user's computer" while finding the NIT did not constitute a tracking device), *with United States v. Jean*, 207 F. Supp. 3d at 942-43 (W.D. Ark. Sept. 13, 2016) (finding the NIT's installation occurred in Virginia when the defendant virtually traveled there); *Matish*, 193 F. Supp. 3d at 612 (finding that, "whenever someone entered Playpen, he or she made, in computer language, 'a virtual trip' via the Internet to Virginia"). Courts within this circuit have largely concluded the NIT Warrant did not comply with Rule 41(b)(4). *Perdue*, 2017 WL 661378, at *3 (relying upon *Michaud*'s reasoning); *Pawlak*, 2017 WL 661371, at *5 (same); *Torres*, 2016 WL 4821223, at *5 (same); *United States v. Rivera*, Eastern District of Louisiana Case No. 2:15-cr-266-CJB-KWR, Dkt. 69 at 13-16. *But see United States v. Smith*, Southern District of Texas Case No. 4:15-cr-467, Dkt. 41 at 11-15 (finding the NIT Warrant complied with Rule 41(b)(4)).[4] Indeed, in each of the Northern and Western Districts of Texas, the courts have reviewed and rejected the very same "tracker" argument presented here by the Government to assert that Rule 41 applies to the NIT Warrant. The Court similarly finds the Government's expansive interpretation of Rule 41(b)(4)'s terms unpersuasive. *See Perdue*, 2017 WL 661378 (citing *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 169 (1977)). To begin, the NIT Warrant itself makes clear it permits searches "of computers that access [Website A]" [Dkt. 25, Ex. 2] and that it authorizes "use of [the NIT] to be deployed on the computer server [in Virginia], obtaining information . . . *from the activating computers* . . ."

[4] Moreover, as to the broader question of whether the NIT Warrant issued in accord with Rule 41's strictures, the majority of courts have found that it did not. *Taylor*, 2017 WL 1437511, at *5 (collecting cases and noting that, as of April 24, 2017, twenty-two courts have found the NIT Warrant violates Rule 41(b), while twelve have found otherwise).

notwithstanding the computers' respective locations [Dkt. 25, Ex. 2, Attachment A]. Moreover, the attached affidavit's description of the NIT's function shows that the property to be searched is the "activating computer," not the user's ethereal digital presence [*see, e.g.*, Dkt. 25, Ex. 2 at 24 (noting that "websites send content to visitors[,]" that the "user's computer downloads that content[,]" that the NIT "augment[s]" such content, and that, once downloaded, the NIT "cause[s] the user's 'activating' computer to transmit certain information" back to the government)].

The Government's analogy to the tracking device in *United States v. Knotts*, 460 U.S. 276 (1983), further exposes Rule 41(b)(4)'s limitations in the NIT context. In *Knotts*, police officers installed a beeper in a drum of chloroform hoping to trace the defendant's movements after he purchased the chemical. 460 U.S. at 278-79. The government did so without any warrant but with the chemical company's consent. *Id.* The beeper acted as a tracking device of which the defendant, in essence, took control when he purchased the chloroform to manufacture a controlled substance in violation of federal law. *Id.* The U.S. Supreme Court held the government's use of this tracking device did not "invade any legitimate expectation of privacy" on the defendant's part because the government's use of the beeper "amounted principally to the following of an automobile on public streets and highways"—something "[a] police car following [the defendant] *could have observed*" anyway. *Id.* at 281, 285. By contrast, here, Agent MacFarlane's Affidavit indicates it is unlikely the FBI would have been able to identify Defendant without the NIT [*see* Dkt. 25, Ex. 1 at 19 (observing that, even with Website A's server in hand, the Government could not identify the website's users without using the NIT)].

Additionally, if the FBI installed the NIT on the Website A server in the Eastern District of Virginia (as the Government contends), and the Government maintained control of that server throughout the investigation, it is unclear how the NIT could have "tracked" Defendant's

movements in any way contemplated under Rule 41(b)(4).[5] The *Michaud* court found that construing the NIT Warrant to fall within the parameters of Rule 41(b)(4) would stretch the Rule too far and noted that,

> [i]f the "installation" occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because Mr. Michaud never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on Mr. Michaud's computer, applying the tracking device exception again fails, because Mr. Michaud's computer was never physically located within the Eastern District of Virginia.

Michaud, 2016 WL 337263, at *6. Although the Court must read Rule 41 broadly, the Court "cannot render it meaningless." *Pawlak*, 2017 WL 661371, at *5 (citing *N.Y. Tel. Co.*, 434 U.S. at 169); *see also United States v. Adams*, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016) (noting "the NIT does not track, it searches[,]" and rejecting the government's *Knotts* analogy); *Perdue*, 2017 WL 661378, at *3 (implying that applying the "tracking device" analogy to the NIT would render Rule 41's geographical limitations meaningless); *Torres*, 2016 WL 4821223, at *5 (rejecting the "tracking device" analogy); *Rivera*, Eastern District of Louisiana Case No. 2:15-cr-266-CJB-KWR, Dkt. 69, at 15-16 (same). Accordingly, as the Court finds the Government's tracking device analogy unpersuasive, the Court concludes that the NIT Warrant issued in violation of Rule 41.[6]

---

[5] Some courts have observed the FBI could have placed a server hosting Website A in every judicial district in the nation and could have then procured valid warrants under Rule 41(b) in every judicial district. *E.g.*, *Vortman*, 2016 WL 7324987, at *11 (citing *United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436, at *7 (C.D. Cal. Aug. 8, 2016)). Although this observation dispatches concerns about the installation question and/or potentially makes other Rule 41(b) subsections applicable, it fails to address how the NIT constitutes a "tracking device," and the Court remains convinced that the NIT does not.

[6] As an aside, the Court notes Defendant's argument concerning the recent amendment of Rule 41 bolsters, rather than weakens, the Government's position. As the *Torres* court concluded regarding this amendment (and the Government's efforts to procure it), "the instant NIT warrant has brought to light the need for Congressional clarification regarding a magistrate's authority to issue a warrant in the internet age, where the location of criminal activity is obscured through the use of sophisticated systems of servers designed to mask a user's identity." 2016 WL 4821223, at *7. In light of this recognized ambiguity, the Government's characterization of the NIT as a tracking device is at least plausible, even if not wholly convincing. *See Vortman*, 2016 WL 7324987, at *12.

B. Effect of Noncompliance with Rule 41

Suppression does not automatically result, however, where a warrant violates Rule 41(b). *Pawlak*, 2017 WL 661371, at *5. Instead, the Fifth Circuit has held that, in the Rule 41 context,

> where there is no constitutional violation nor prejudice in the sense that the search would likely not have occurred or been as abrasive or intrusive had Rule 41 been followed, suppression . . . is not appropriate if the officers concerned acted in the affirmative good faith belief that the warrant was valid and authorized their conduct.

United States v. Comstock, 805 F.2d 1194, 1207 (5th Cir. 1986). In other words, a defendant must establish that the warrant issued in violation of Rule 41 was unconstitutional and/or prejudiced the defendant. *See id.* If the defendant fails to establish either, the violation is technical and the defendant must show that the officers involved lacked a good faith belief the warrant was valid or that it authorized their actions. *See id.*

Defendant argues the Eastern District of Virginia Magistrate's failure to comply with Rule 41 in issuing the NIT Warrant requires suppression of the evidence obtained in this case [Dkt. 25 at 10-16]. Defendant first contends the Rule 41 violation "implicates [§] 636(a)," which imposes jurisdictional limitations on the powers of magistrate judges, and that the Rule 41 violation is accordingly *per se* harmful [Dkt. 25 at 10-11]. Defendant also asserts the Rule 41 violation prejudiced him because the Residential Warrant would not have issued "but for information derived from the improperly issued NIT Warrant" [Dkt. 25 at 11-14]. The Government argues that any violation of Rule 41 is merely a "technical" error that does not mandate suppression [Dkt. 38 at 14-18].

1. Impact of § 636

Defendant cites the concurring opinion in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), in support of his assertion that a violation of § 636 (vis-à-vis a Rule 41 violation) is *per*

se harmful. Defendant contends the "violation of [this] jurisdictional statute mandates suppression to preserve judicial integrity and proper separation of powers" [Dkt. 25 at 10-11]. The Court disagrees. First, Defendant cites no authority in the Fifth Circuit dictating that a § 636 violation in the issuance of a warrant is *per se* harmful to a criminal defendant or otherwise undermines the defendant's Fourth Amendment rights. Moreover, in its own research, the Court has found that a violation of § 636 does not necessarily implicate a defendant's Fourth Amendment rights. Specifically, district courts in this circuit have found:

> The Fourth Amendment does not address the powers of magistrate judges or district judges, nor does it address whether judges' power extends beyond district boundaries. The Fourth Amendment simply requires, in pertinent part, that a warrant be issued by a "neutral magistrate." . . . Thus any more specific restrictions regarding who can issue a particular type of warrant are statutory or rule creations that do not implicate the Fourth Amendment.

Perdue, 2017 WL 661378, at *4 (citations omitted); *see also Pawlak*, 2017 WL 661371, at *6 (rejecting argument that Rule 636 violation *per se* requires suppression); *Torres*, 2016 WL 2821223, at *7 (finding "the violation of Rule 41(b)(4) did not have a Constitutional dimension" when evaluating the NIT Warrant); *Deichert*, 2017 WL 398370, at *8 (noting that "the Fourth Amendment imposes two jurisdictional requirements upon any authority exercising power to issue a warrant: the authority must be a magistrate, and the magistrate must be neutral and detatched[,]" neither of which speak to Rule 41's geographical limitations).

Further, and as the U.S. Supreme Court has held time and again, the exclusionary rule exists to deter bad police conduct, not to prevent judicial errors. *See, e.g.*, *Arizona v. Evans*, 514 U.S. 1, 15 (1995) (finding "[a]pplication of the *Leon* framework supports a categorical exception to the exclusionary rule for clerical errors of court employees"); *Davis v. United States*, 564 U.S. 229, 240-41 (2011) (finding exclusion inappropriate where police relied upon erroneous appellate precedent and noting exclusion in such case would only act to penalize judicial error). The logical

end to Defendant's argument here (that a § 636 violation automatically counsels suppression) is suppression on the basis of a perceived judicial error, namely the Eastern District of Virginia Magistrate's issuance of the NIT Warrant without statutory authority. As the foregoing authorities illustrate, however, the U.S. Supreme Court has foreclosed such argument, and other courts in this circuit have rejected it outright. Moreover, Rule 41 is ambiguous in this context: while some courts have found the NIT Warrant was issued in violation of Rule 41(b) (and § 636), others have found just the opposite. *Compare Perdue*, 2017 WL 661378, at *3, *with Smith*, Southern District of Texas Case No. 4:15-cr-467, Dkt. 41 at 11-15. Still others have rejected the Government's tracking device theory but have found the theory at least is credible. *See Vortman*, 2016 WL 7324987, at *12 (collecting cases). To find the violation here amounts to one of constitutional dimension would fly in the face of this recognized ambiguity in the Rule and, by extension, § 636. Accordingly, the Court finds issuance of the NIT Warrant in violation of Rule 41 (and consequently of § 636) does not, standing alone, require suppression or amount to a constitutional violation. *See Torres*, 2016 WL 4821223, at *7.[7]

2. Prejudice

Defendant further contends he "was prejudiced because the search authorized by the Residential Warrant would never have occurred but for information derived from the improperly issued NIT Warrant" [Dkt. 25 at 11-12]. Specifically, Defendant asserts that, were it "not for the NIT Warrant, there would have been no probable cause to support the Residential Warrant" [Dkt. 25 at 12].[8] Defendant seemingly relies upon *United States v. Glover*, 736 F.3d 509, 510-16 (D.C. Cir. 2014), to support this argument,[9] and asserts that, while "[t]he agents in *Glover* could

[7] See also the Court's discussion *supra* at **Section III.A**.
[8] The Court notes Defendant does not argue the NIT Warrant issued without probable cause.
[9] To the extent Defendant argues through his citation to *Glover* that the alleged jurisdictional defect warrants suppression, the Court finds this argument unavailing. *See supra* **Sections III.A.** and **III.B**.

have simply obtained the warrant from a magistrate judge in [the proper district,] in this case there is no magistrate judge with authority to issue the nationwide warrant" [Dkt. 25 at 12-13]. The Government argues Defendant did not suffer prejudice because, whether or not the Eastern District of Virginia Magistrate had authority under Rule 41 to issue the NIT Warrant, a district judge certainly would have had authority to issue the NIT Warrant [Dkt. 38 at 15].[10]

To demonstrate "prejudice" as contemplated under *Comstock*, which distinguished between prejudicial (or constitutional) and non-prejudicial (or technical) violations of Rule 41, a defendant must show that "the search would likely not have occurred or been so abrasive or intrusive had Rule 41 been followed[] . . . ." 805 F.2d at 1207. If a search could have occurred and "the evidence . . . could have been available by other lawful means," a defendant has suffered no prejudice. *Michaud*, 2016 WL 337263, at *6 (citing *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980)). Here, although no other federal magistrate judge would have had authority to issue a warrant that reaches outside of the magistrate's district in the manner contemplated by the NIT Warrant, the FBI could have petitioned a district judge for the same warrant. In other words, the Government had at least one other lawful means through which to obtain the evidence against Defendant. Defendant's citation to *Glover* fails for this reason. As Defendant points out, the Government could have avoided the D.C. Circuit's ruling against it in *Glover* by petitioning a judge in a different district for the warrant it sought. *Cf. Glover*, 736 F.3d at 510-16 (interpreting Title III of the Omnibus Crime Control and Safe Streets Act of 1968). Rule 41 generally does not

[10] Defendant argues, as well, that the Government's failure "to provide notice of the NIT search within 30 days of the search of [Defendant's] computer" prejudiced Defendant [Dkt. 25 at 11]. The Government notes, however, that the NIT Warrant "was sealed by court order until approximately March 21, 2016"—months after the execution of the Residential Warrant in November 2015—and, in any event, that the NIT Warrant and other relevant documents "were produced to [Defendant] as part of discovery" once Defendant was indicted [Dkt. 38 at 14 n.7]. Defendant does not show how he suffered prejudice as a result of receiving these materials when he did. Accordingly, the Court finds Defendant has failed sufficiently to allege that the Government's failure to provide notice by a particular time amounts to prejudice as contemplated under *Comstock*.

constrain district judges when they issue warrants, and numerous courts (including the Northern District of Texas) have relied on this principle in finding that defendants whose information the NIT captured in the FBI's investigation suffered no prejudice by and through the Eastern District of Virginia Magistrate's issuing the NIT Warrant. *See, e.g.*, *Perdue*, 2017 WL 661378, at *4 (finding that, "had a district judge been presented the same warrant application, the district judge would have been authorized to issue a warrant for the search"); *Pawlak*, 2017 WL 661371, at *6 (same); *United States v. Hammond*, --- F. Supp. 3d ---, 2016 WL 7157762, at *5 (N.D. Cal. 2016) (same); *see also Jean*, 207 F. Supp. 3d at 936 n.16 (noting "[d]istrict judges are not limited by Rule 41(b) as magistrate judges are"). Because the Government could have petitioned a district judge for the NIT Warrant, the Court likewise finds Defendant did not suffer prejudice here.

Because the Court has determined the Eastern District of Virginia Magistrate issued a deficient warrant that neither implicates Defendant's constitutional rights nor prejudices Defendant, the Court concludes the violation is technical. The Court accordingly turns to consider whether good faith exception applies. *See Payne*, 341 F.3d at 399 (citing *Leon*, 468 U.S. at 921-25); *see also Perdue*, 2017 WL 661378; *Pawlak*, 2017 WL 661374.

IV. GOOD FAITH AND *LEON* EXCEPTIONS

Finally, Defendant argues the good faith exception cannot apply here because "the officers acted in intentional and deliberate disregard of Rule 41" in requesting and executing the NIT Warrant [Dkt. 25 at 14-17]. Defendant contends "it is evident from the plain language of Rule 41(b) that no interpretation would allow the search of potentially thousands of computers located outside the authorizing district" and that, in any event, the Government knew as early as May 5, 2014, that no such warrant could issue under Rule 41(b)'s terms [Dkt. 25 at 14-15]. In this vein, Defendant asserts the Government's proposed amendment to Rule 41(b) and the

memorandum accompanying it show that the Government understood that accommodating such a warrant under Rule 41 would require "an entirely new subsection to Rule 41(b), rather than a clarification to an existing subsection" [Dkt. 25 at 15].

Within the Fourth Amendment framework, the Court remains at step one: determining whether the good faith exception or any of the *Leon* exceptions applies. *See Leon*, 468 U.S. at 924. To reiterate, even evidence obtained under a deficient warrant "is admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith." *Payne*, 341 F.3d at 399. Generally an officer's reliance meets this standard unless "a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *Pope*, 467 F.3d at 916 (citations and internal quotations omitted). Nevertheless, the issuance of a warrant by a magistrate typically suffices to establish an officer's good faith, *Pena-Rodriquez*, 110 F.3d at 1130, though good faith cannot be established if one of the four *Leon* exceptions applies, *see Payne*, 341 F.3d at 399-400.[11] Importantly, the officers' subjective belief regarding the validity of the warrant does not enter this analysis. *See Leon*, 468 U.S. at 922 n.23. Rather, courts confine the inquiry "to the objectively ascertainable question of whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.*

The Court agrees with the argument advanced by the Government in this instance that "it was far from clear at the time [the NIT Warrant was issued] that the NIT Warrant violated Rule 41(b)" [Dkt. 38 at 21]. While this Court concludes (as more than twenty other courts have) that the Eastern District of Virginia Magistrate issued the NIT Warrant without authority under Rule

[11] Defendant does not expressly argue that any of the *Leon* Exceptions applies in this case. To the extent Defendant argues the fourth *Leon* Exception (regarding the NIT Warrant's particularity) applies, the Court finds it does not. *See supra* **Section II**.

41, at least twelve courts have found to the contrary. *Taylor*, 2017 WL 1437511, at *3-4 (collecting and categorizing cases ruling on the issue). These diverging opinions concerning the scope of Rule 41(b) as applied to the NIT Warrant demonstrate that an objectively reasonable, well-trained officer could have concluded (at the times the FBI applied for and executed the NIT Warrant) that Rule 41(b) either did or did not authorize such a warrant. *See Perdue*, 2017 WL 661378, at *5 (relying on the fact that "several courts have held that NIT Warrant did not violate Rule 41(b)" in "conclud[ing] that the government did not intentionally violate the Rule"); *Pawlak*, 2017 WL 661374, at *6 (same). Further, Defendant's allegations concerning the Government's advocacy for a rule change prior to and during its application for and execution of the NIT Warrant has no bearing on whether the good faith exception applies here: the Government's advocacy reveals its subjective beliefs about Rule 41's scope, not the objective reality. *See Perdue*, 2017 WL 661378, at *5 ("Regardless of the agents' subjective beliefs and the existence of potentially contrary, albeit non-binding, authority, it was far from clear at th[ose] time[s] that the NIT Warrant violated Rule 41(b)"); *Pawlak*, 2017 WL 661374, at *6 (same).

Moreover, and as noted *supra*, the exclusionary rule exists to deter bad police conduct. *See, e.g.*, *Evans*, 514 U.S. at 15; *Davis*, 564 U.S. at 240-41. In the present case, though, "to the extent a mistake was made . . . , it was not made by the agents . . . [but was instead] made by the [Eastern District of Virginia Magistrate] when she mistakenly issued a warrant outside her jurisdiction." *United States v. Werdene*, 188 F. Supp. 3d 431, 452 (E.D. Pa. 2016). Indeed, in the instant case, Defendant asserted at Hearing the officers involved in seeking the NIT Warrant consulted with Department of Justice attorneys prior to approaching the Eastern District of Virginia Magistrate [Dkt. 46 at 8]. *See Werdene*, 188 F. Supp. 3d at 452-53 (noting officer consultation with government attorneys prior to seeking a warrant is to be encouraged). Further,

Defendant's assertions at Hearing about improper behavior on the part of the officers seeking the NIT Warrant are belied by both the contents of the NIT Warrant and the attachments thereto, which demonstrate that Agent MacFarlane explained thoroughly to the Eastern District of Virginia Magistrate how the NIT would function and that Agent MacFarlane expressly requested that the NIT Warrant authorize search of "an activating computer—wherever located" [Dkt. 25, Ex. 2 at 23-27, 29]. *See Werdene*, 188 F. Supp. 3d at 452-53. "Exclusion of the evidence [here, which the officers] seized pursuant to the NIT [W]arrant[,] would serve little deterrent purpose where the mistaken conduct of the magistrate judge, not the officers, invalidated the warrant." *Taylor*, 2017 WL 1437511, at *16. Accordingly, the Court finds the good faith exception applies here and that, as a result, Defendant's Motion to Suppress Evidence [Dkt. 25] should be denied.

MOTION FOR EVIDENTIARY HEARING

Defendant also moves for an evidentiary hearing because, Defendant asserts, the Motion to Suppress presents "factual issues which are contested between the parties" and "the issue of whether or not the agents seeking the [NIT Warrant] knew they were seeking a search warrant authorization from a Magistrate Judge for a search outside the scope of the judge's authority" [Dkt. 41]. The Government opposes this motion [Dkt. 41]. Regarding evidentiary hearings incident to a motion to suppress, the Fifth Circuit has held as follows:

> Evidentiary hearings are not granted as a matter of course, but are held only when the defendant alleges sufficient facts which, if proven, would justify relief. . . . Factual allegations set forth in the defendant's motion, including any accompanying affidavits, must be "'sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.'" . . . General or conclusionary assertions, founded upon mere suspicion or conjecture, will not suffice. . . .
>
> Inherent in these flexible guidelines is a judicial recognition that "the determination of whether a hearing is required [on a motion to suppress] is necessarily dependent upon the particular facts which attend a particular request, and the district court is properly left with a certain amount of discretion in this regard."

United States v. Harrelson, 705 F.2d 733, 737 (5th Cir. 1983) (citations omitted). The Court has evaluated Defendant's allegations in detail and has exhaustively examined the attachments Defendant proffers in support of the Motion to Suppress. As a result of its review of the record and of the representations at Hearing, the Court has concluded the good faith exception applies in this case. The Court reaches this conclusion because Defendant's allegations against a finding of good faith center entirely on Defendant's desire to ascertain the subjective beliefs of the officers involved, not on what a reasonably well-trained officer objectively would have known or on the applicability of any of the *Leon* Exceptions. Thus, as numerous other courts have held, this Court also holds that no additional information or testimony on the matters identified in Defendant's allegations in the Motion to Suppress, the Motion for Evidentiary Hearing, or at Hearing would preclude application of the good faith exception. *See, e.g.*, *United States v. Ammons*, 207 F. Supp. 3d 732 (W.D. Ky. 2016) (denying without evidentiary hearing defendant's motion to suppress by applying good faith exception); *Michaud*, 2016 WL 337263 (same); *United States v. Gaver*, No. 3:16-cr-88, 2017 WL 1134814 (S.D. Ohio Mar. 27, 2017) (denying defendant's request for evidentiary hearing); *Pawlak*, 2017 WL 661371, at *1 n.2 (same); *see also Anzalone*, 208 F. Supp. 3d 358 (denying defendant's motion to suppress without evidentiary hearing); *United States v. McLamb*, --- F. Supp. 3d ---, 2017 WL 243987 (E.D. Va. Jan. 19, 2017) (same).[12] As a result, Defendant fails to allege sufficient facts that, if proved, would justify relief. Accordingly, the Court recommends that Defendant's Motion for Evidentiary Hearing be denied [Dkt. 41].

[12] The Court also notes that, if any error was made, it was judicial error, not the FBI's or the Government's. *See supra* **Section IV**.

CONCLUSION AND RECOMMENDATION

Based on the foregoing, the Court recommends Defendant Jose Victor Hernandez-Cuellar's Motion to Suppress Evidence [Dkt. 25] and Opposed Motion Requesting Evidentiary Hearing [Dkt. 41] each be **DENIED**.

Within fourteen days after entry of the magistrate judge's report, any party must serve and file specific written objections to the findings and recommendations of the magistrate judge. 28 U.S.C. § 636(b)(1)(C). In order to be specific, an objection must identify the specific finding or recommendation to which objection is made, state the basis for the objection, and specify the place in the magistrate judge's report and recommendation where the disputed determination is found. An objection that merely incorporates by reference or refers to the briefing before the magistrate judge is not specific.

Failure to file specific, written objections will bar the party from appealing the unobjected-to factual findings and legal conclusions of the magistrate judge that are accepted by the district court, except upon grounds of plain error, provided that the party has been served with notice that such consequences will result from a failure to object. *See Douglass v. United Servs. Auto. Ass'n*, 79 F.3d 1415, 1417 (5th Cir. 1996) (en banc), *superseded by statute on other grounds*, 28 U.S.C. § 636(b)(1) (extending the time to file objections from ten to fourteen days).

SIGNED this 1st day of May, 2017.

Christine A. Nowak
UNITED STATES MAGISTRATE JUDGE